3. What are the different script categories in NSE?

The **Nmap Scripting Engine (NSE)** organizes its scripts into categories based on their functionality and intended use. These categories help users quickly identify the type of script needed for their tasks.

---

1. Auth

- **Purpose**: Authentication-related tasks.
- **Examples**: Brute-forcing credentials, testing default logins, and bypassing authentication mechanisms.
- **Use Case**: Verify if a service uses weak or default passwords.
  - Example Scripts:
    - `ssh-brute`: Attempts to brute-force SSH logins.
    - `ftp-anon`: Checks for anonymous FTP login.

---

2. Broadcast

- **Purpose**: Discover hosts and services on the same local network.
- **Examples**: Scanning for network resources like printers, shared files, or streaming devices.
- **Use Case**: Perform network inventory in a LAN environment.
  - Example Scripts:
    - `broadcast-dhcp-discover`: Sends DHCP discover requests.
    - `broadcast-netbios-master-browser`: Lists hosts from the master browser on Windows networks.

---

3. Bruteforce

- **Purpose**: Perform password-guessing attacks.
- **Examples**: Target services such as SSH, FTP, HTTP, and databases.
- **Use Case**: Assess resilience to brute-force attacks.
  - Example Scripts:
    - `http-brute`: Brute-forces web login forms.
    - `mysql-brute`: Brute-forces MySQL logins.

---

4. Discovery

- **Purpose**: Gather information about a target host or network.
- **Examples**: Identifying services, subdomains, or users.
- **Use Case**: Enhance reconnaissance by uncovering hidden resources.
    - Example Scripts:
        - `dns-brute`: Performs DNS brute-forcing.
        - `snmp-brute`: Queries SNMP devices for information.

---

5. Intrusive

- **Purpose**: Perform scans or tests that may negatively affect the target.
- **Examples**: Stress testing, exploiting vulnerabilities, or aggressive scanning.
- **Use Case**: Validate vulnerabilities or test service resilience.
    - Example Scripts:
        - `http-sql-injection`: Tests for SQL injection vulnerabilities.
        - `smtp-brute`: Attempts to brute-force SMTP credentials.

---

6. Malware

- **Purpose**: Detect malware-infected hosts or malicious services.
- **Examples**: Analyzing payloads or identifying botnet command-and-control servers.
- **Use Case**: Detect compromised devices in a network.
    - Example Scripts:
        - `http-malware-host`: Checks if a host is serving malware.
        - `irc-botnet-channels`: Detects botnet activity on IRC servers.

---

7. Safe

- **Purpose**: Scripts that are unlikely to harm or disrupt the target.
- **Examples**: Basic information gathering or non-intrusive vulnerability checks.
- **Use Case**: Run scans on production systems without risking downtime.
    - Example Scripts:
        - `banner`: Retrieves application banners.
        - `ssl-cert`: Retrieves SSL certificate details.

---

8. Version

- **Purpose**: Identify software versions and associated information for services.
- **Examples**: Checking version numbers to identify vulnerabilities.
- **Use Case**: Map versions to known CVEs or advisories.

  - Example Scripts:
    - `http-server-header`: Fetches HTTP server headers.
    - `ftp-vsftpd-backdoor`: Checks for a specific backdoor in VSFTPD.

---

9. Vulnerability (Vuln)

- **Purpose**: Identify known vulnerabilities in services or configurations.
- **Examples**: Scanning for CVEs, misconfigurations, or outdated software.
- **Use Case**: Quickly assess the security posture of a target.
  - Example Scripts:
    - `smb-vuln-ms17-010`: Checks for EternalBlue (MS17-010) vulnerability.
    - `http-dombased-xss`: Detects DOM-based XSS vulnerabilities.

---

10. Exploit

- **Purpose**: Actively exploit vulnerabilities in a service.
- **Examples**: Gaining unauthorized access or escalating privileges.
- **Use Case**: Penetration testing to demonstrate risk.
  - Example Scripts:
    - `ftp-proftpd-backdoor`: Exploits a backdoor in ProFTPD.
    - `http-shellshock`: Exploits the Shellshock vulnerability.

---

11. External

- **Purpose**: Leverage external services or databases for information.
- **Examples**: Querying WHOIS or online APIs.
- **Use Case**: Enrich scan results with external data.
  - Example Scripts:
    - `whois-domain`: Queries WHOIS information for domains.
    - `ip-geolocation-geoplugin`: Finds geolocation information for an IP address.

---

12. Fuzzer

- **Purpose**: Send unexpected or random data to a target to identify bugs or vulnerabilities.
- **Examples**: Stress-testing applications or finding unhandled inputs.
- **Use Case**: Identify security weaknesses in applications or protocols.
  - Example Scripts:
    - `http-fuzz`: Fuzzes HTTP inputs.

    - `dns-fuzz`: Fuzzes DNS services.

Summary of Script Selection

To run specific categories or combine multiple:

```
nmap --script <category1>,<category2> <target>
```

Example: Run safe and vuln scripts:

```
nmap --script safe,vuln <target>
```